

FILED _____
LOGGED AL ENTERED
RECEIVED
AUG 06 2019
AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY DEPUTY

**IN THE MATTER OF THE SEARCH
OF**

**INFORMATION CONTAINED IN OR
ASSOCIATED WITH THE ACCOUNTS
LISTED IN ATTACHMENTS A-1, A-2, A-
3, AND A-4 AND WITHIN THE
POSSESSION AND/OR CONTROL OF
APPLE, INC. AND GOOGLE LLC.**

CASE NO. _____
AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND

19-2432 JMC

19-2435 JMC

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Special Agent Brendan Plasha, being duly sworn, depose and state that:

PURPOSE OF THE AFFIDAVIT

1. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Apple and Google, respectively, to disclose to the government records and other information in their possession, pertaining to the accounts listed below and including information related to subscriber or customer operating said accounts:

- a. mcfaddenkelvin1993@icloud.com (Attachment A-1 and B-1);
- b. mcfaddenkelvin1993@gmail.com (Attachment A-2 and B-2);
- c. mcfaddenlijah2012@gmail.com (Attachment A-3 and B-3);
- d. slw30@gmail.com (Attachment A-4 and B-4).

2. As will be explained below, the accounts listed in paragraph 1(a) through 1(c) are linked and associated with Kelvin McFadden. The account listed in paragraph 1(d) is linked and associated with Stewart Williams.

3. The United States has probable cause to believe that the sought after records and other information associated with the accounts will provide evidence of violations of 18 U.S.C. §1951(a) (Affecting Interstate Commerce by Robbery).

19-2432 JMC -

19-2435 JMC

DAL

JURISDICTION

4. This Court has jurisdiction to issue the requested warrants because it is “a court of competent jurisdiction” as defined in 18 U.S.C. § 2711. *See* 18 U.S.C. § 2703(c)(1)(A). Specifically, the Court is “a district court of the United States (including a magistrate judge of such court) . . . that--has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

AGENT BACKGROUND

5. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (“ATF”), and have been since 2015. I am currently assigned to the ATF Baltimore Field Division, Baltimore Field Office. I attended the United States Department of Homeland Security’s Criminal Investigator Training Program and ATF’s Special Agent Basic Training, both located in Glynco, Georgia, for a combined period of twenty-six weeks. I have received extensive training, both formal and on-the-job, in the provisions of the Federal Firearms Laws and Federal Narcotics Laws administered under Title 18, Title 21, and Title 26 of the United States Code. As an ATF agent, I have conducted and participated in numerous investigations concerning violations of federal firearm laws, violations of federal controlled substance laws, and the commission of violent crimes. I have received specialized training regarding, and have personally participated in, various types of investigative activities, including: (a) physical surveillance; (b) the debriefing of defendants, witnesses, informants, and other individuals who have knowledge concerning violations of federal firearms and controlled substance laws; (c) undercover operations; (d) the execution of search warrants; (e) the consensual monitoring and recording of conversations; (f) electronic surveillance through the use of pen registers and trap and trace devices; (g) the court-authorized interception of both wire and electronic communications (i.e., Title III wiretaps); and (h) the handling,

19-2432 JMC -

19-2435 JMC

DAL

maintenance, and examination of evidence, including wireless telephones and computers.

6. As a Special Agent with the ATF, I am authorized to investigate violations of laws of the United States and as a law enforcement officer with the authority to make arrests and execute warrants issued under the authority of the United States.

7. The information contained in this affidavit comes from my personal observations, my training and experience, and information obtained from other agents, police officers and detectives, witnesses, documents, records, and reports. Since this affidavit is being submitted for the limited purpose of establishing probable cause for securing the search warrant, I have not included every fact known to me concerning the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of 18 U.S.C. § 1951(a) (Robbery Affecting Commerce) will be found in the sought after records and other information associated with the accounts.

BACKGROUND ON ICLOUD

8. I know that Apple is an American multinational corporation that designs, develops, and sells consumer electronics, computer software and personal computers.

9. I also know that Apple offers services called “iCloud” and “iMessage” to its users.

10. iCloud is a service provided by Apple that allows its users to store files on Apple’s servers in order to sync their files across all of their Apple devices. According to iCloud’s terms and conditions, at <http://www.apple.com/legal/internet-services/icloud/en/terms.html>, iCloud collects and stores “your last three backups.” “Backup is limited to device settings, device characteristics, photos and videos, documents, messages (iMessage, SMS, and MMS), ringtones, app data (including Health app data), location settings (such as location-based reminders that you have set up), and Home screen and app organization.”

11. Additionally, for device-based location information, iCloud “must collect, use,

19-2432 JMC -

19-2435 JMC

DAL

transmit, process and maintain your location data, including but not limited to the geographic location of your device and information related to your iCloud account (“Account”) and any devices registered thereunder, including but not limited to your Apple ID, device ID and name, and device type.” Anyone using an iPhone, must set up an Apple ID, using a valid electronic mail address. An iPhone typically has a cellular telephone number associated with it, as well as cellular telephone service provided by a third-party cellular company.

12. Messaging, the transmission of information from one electronic device to another, comes in many variations. I know based on training and experience that individuals involved in collective criminal activity use Apple devices to send messages to each other, including iMessages, which are discussed in further detail below.

13. Traditional text messaging, formally known as the Short Message Service (“SMS”), is text-only service provided by a mobile telephone service provider. This service is normally provided over the cellular network, from one device to another, based on mobile telephone number. SMS has been augmented with the Multimedia Messaging Service (“MMS”) which expands the capabilities with group messaging and expanded message formats. Group messaging allows individuals to communicate with multiple people simultaneously, while expanded message formats allow users to transmit pictures, videos and/or audio recordings. Further, based on the typically larger sizes of these messages, MMS is normally delivered over a user’s mobile data connection rather than the mobile telephone, or circuit, connection. Mobile telephone service providers typically maintain transactional records regarding SMS and MMS communications, including the sender, recipient, and date/time of the message.

14. Apple has further evolved messaging with iMessage. Using the Messages application on any Apple device that uses Apple iOS or Mac OS X, a user can send an iMessage to any other iOS or Mac OS X device. Further, iMessages sent from one Apple device can appear on

19-2432 JMC - 19-2435 JMC

DAL

all other Apple devices that are associated with the same Apple ID, and have activated the Messages application on that device. An iMessage is sent and received based on an Apple ID, but can also be sent based on the user's telephone number, if a telephone number is associated with that device. If an iMessage is sent, the message uses an Internet data connection, whether that connection is provided by the mobile telephone service provider or a Wi-Fi hotspot. Apple encrypts iMessages. I am aware that iMessages is the default messaging application for iPhones, unless the user affirmatively disables the iMessages application.

15. If a data connection is not available to the Apple device, or the Apple device is sending a message to a non-Apple device, the Messages application will default to traditional SMS if possible for delivery of the message. Further, iOS allows a user of Apple devices to disable iMessage on one or more of a user's Apple devices, so that the user will not receive iMessages on a given device. Transactional records pertaining to iMessages sent and received are not captured through the mobile telephone service provider. However, Apple does capture transactional records regarding iMessages.

16. Based on my training and experience, I have learned that iPhones often have associated "Cloud" (Backup) accounts on which there is data and information stored by the user of the iPhone. Moreover, based on my training and experience, I know that instant messages, emails, voicemails, photos, and videos—all of which may be saved on a user's iCloud account—are often created and used in furtherance of collective criminal activities, including firearm and drug trafficking offenses.

BACKGROUND ON GOOGLE ACCOUNTS

17. Google provides numerous free services to the users with a Google account. Some of services include, Gmail, YouTube, Voice, Blogger, Google+, Hangouts, Android, Photos, Drive, Location History, and Search and Browsing History. Gmail is a web based email service. YouTube

19-2432 JMC - 19-2435 JMC

DAL

is a free video sharing website that allows users upload, view and share videos. Voice is Google's calling, voicemail transcription, and text messaging service. Blogger is Google's free weblog publishing tool for sharing text, photos, and video. Google+ is a forum to share photos, videos, and other information with other users. Android is Google's open source operating system used for mobile devices. Photos stores images for a broad range of Google products. Drive is Google's online storage service for a wide range of file types.

18. I know from my training and experience that records and information recovered from Google Accounts can provide valuable evidence of crimes. For example with respect to affecting interstate commerce by robbery, location, search, and browsing history can provide evidence in the form of showing that a Target searched for information associated with a robbery target, or was located near the scene of the robbery. Targets may also search for information related to the sale of stolen merchandise. Additionally, I know that Gmail and Google Hangouts offer chatting functionality that can be used on a mobile device, such as a cellular phone. Such chat function can be used between coconspirators to discuss criminal activities.

PROBABLE CAUSE

19. Between May 25, 2018 and September 1, 2018, there were a total of 18 robberies that occurred in Baltimore City, Baltimore County, and Anne Arundel County that share common characteristics and are linked together by various pieces of evidence. The robberies occurred in geographic and temporal clusters. Additionally, groupings of these robberies appear to have involved similar looking weapons and clothing. There is also forensic evidence, in the form of fingerprints, that link Stewart Williams and Kelvin McFadden to several robberies. Finally, there is surveillance footage of many of these robberies.

20. The below chart lists the entire series of robberies.

19-2432 JMC - 19-2435 JMC

DAL

Date	Business Name	Location
1 5/25/2018	Conrad's Crabs and Seafood Market	1720 E. Joppa Rd, Parkville, MD 21234
2 6/10/2018	Pappas Liquor Store	1725 Taylor Ave, Parkville, MD 21234
3 6/20/2018	Smoothie King	1830 York Rd, Lutherville-Timonium, MD 21093
4 6/20/2018	Padonia Liquors	51 E. Padonia Rd, Lutherville-Timonium, MD 21093
5 6/20/2018	Liquor Mart	833 Taylor Ave, Towson, MD 21286
6 7/10/2018	Group of Individual Victims	1700 Yakona Rd, Baltimore City, MD 21234
7 7/11/2018	Individual Victim	8625 Walther Blvd, Baltimore City, MD 21236
8 7/11/2018	Walther Liquors	8625 Walther Blvd, Baltimore City, MD 21236
9 7/18/2018	Harford Beverage	7732 Harford Rd, Parkville, MD 21234
10 7/20/2018	C-Mart	8039 Fort Smallwood, Riviera Beach, MD 21226
11 7/22/2018	Wawa (attempted)	8300 Veterans Highway, Millersville, MD 21108
12 7/26/2018	8 Days A Week Convenience Mart	1700 Taylor Ave, Parkville, MD 21234
13 8/5/2018	John's Liquor and General Store	812 Duvall Hwy, Pasadena, MD 21122
14 8/18/2018	Quick Stop Food Mart	3301 E Joppa Rd, Parkville, MD 21234
15 8/21/2018	GameStop	3611 Washington Blvd, Halethorpe, MD 21227
16 8/25/2018	GameStop	6901 Security Blvd, Baltimore City, MD 21207
17 8/28/2018	GameStop	1004 Taylor Ave, Towson, MD 21286
18 9/01/2018	GameStop	6370 York Rd, Baltimore, MD 21212

19-2432 JMC - 19-2435 JMC

DAL

21. On June 22, 2018, Michael Arnold was arrested in Anne Arundel County while attempting to rob a Wawa (07/22/2018).

22. After Arnold's arrest, based on Arnold's physical appearance and other evidence, investigators identified multiple robberies of convenience and liquor stores that they believed Arnold and other co-conspirators were responsible for or involved with.

23. Arnold has been charged in Anne Arundel County with the C-Mart robbery (7/20/2018) and the Wawa attempted robbery (7/22/2018). Your affiant understands that Arnold has reached a plea agreement with the state prosecutor for those crimes.

24. After being originally charged by the State of Maryland, on May 30, 2019, a Federal Grand Jury indicted Stewart Williams and Kelvin McFadden with three counts of violating 18 U.S.C. § 1951(a), two substantive counts and a conspiracy count. (JKB-19-0271).

25. On September 1, 2018, Stewart Williams and Kelvin McFadden were arrested in Baltimore City after leading police on a high speed chase following the robbery of a GameStop. That robbery involved the taking of U.S. currency and video game systems. Police were able to track the location of the car using a "cash tracker" that was taken by the robbers amongst cash stolen during the GameStop robbery. Police obtained a search warrant for the car, which they also learned was registered to McFadden. During that search, police recovered numerous pieces of evidence, including the cash tracker, a black BB/replica gun matching the gun used by robbers during the four GameStop robberies, numerous game systems, two hats that matched hats worn by the robbers who had just committed the 9/1/2018 GameStop robbery, and two cell phones. One of the matching hats recovered from the car was a blue hat with a white star. The other hat was a San Antonio Spurs hat. Images of both are below.

19-2432 JMC -

19-2435 JMC

DAL



26. A photograph of the rear portion of the dark-colored Honda Accord that was registered to Kelvin McFadden and searched pursuant to the warrant is below.



27. After the arrest of Williams and McFadden, investigators executed a search warrant for the location to which the pair had fled, an apartment located on 922 N. Stricker Street in Baltimore. Among other items, investigators recovered a burgundy or maroon shirt that was found in a trashcan within the apartment. That shirt matched one worn by one of the robbers during the 9/1/2018 GameStop robbery. A photograph is included below.

FILED
LOGGED
AUG 06 2019
BALTIMORE DISTRICT COURT
OF MARYLAND, CIRCUIT



28. After the arrest of Williams and McFadden, based on their physical appearance and other evidence, investigators identified multiple robberies of stores, convenience stores and liquor stores that they believe Williams and McFadden and certain co-conspirators were responsible for or involved with.

29. For example, investigators reviewed surveillance footage of the robberies of all four GameStops, each of which involved two black males entering and robbing the stores. The appearance of those two robbers was consistent with Stewart Williams and Kelvin McFadden for each GameStop robbery. Still images from surveillance footage captured the robbers as they left the GameStop stores after completing the robberies. Still images of the robbers from the 8/28/2018 and 9/1/2018 GameStop robberies captured photos of the two different robbers wearing what appears to be the same hat during the two different robberies, a blue hat with a white star. A still image from the 9/1/2018 robbery shows one of the robbers, who is wearing a blue hat with a white star, wearing a shirt that matches the one recovered ripped up inside a trash can at 922 N. Stricker Street. Additionally, the San Antonio Spurs hat that was recovered also matches one worn by the two different robbers on different days of GameStop robberies. Some example images are below.



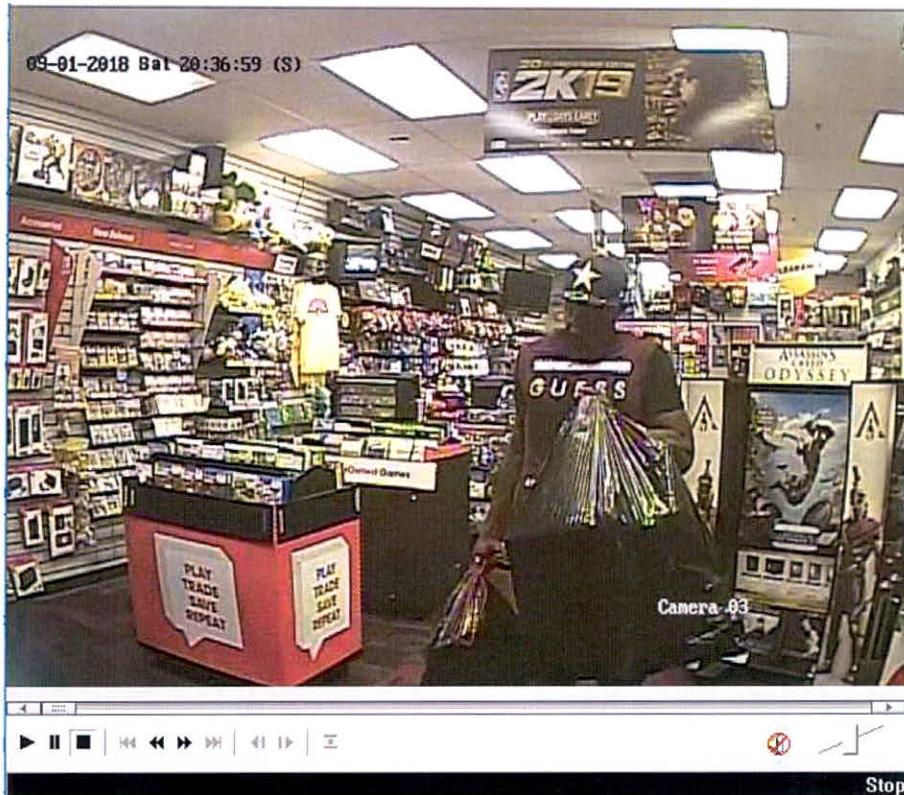
GameStop 8/21/2018 Washington Boulevard, Halethorpe, MD 21227



GameStop 8/28/2018 1004 Taylor Avenue, Towson, MD 21286

19-2432 JMC - 19-2435 JMC

DAL



GameStop 9/1/2018 6370 York Road, Baltimore MD



GameStop 9/1/2018 6370 York Road, Baltimore MD

30. Additionally, relying on the serial number located on a receipt from a pawn store,

investigators were able to determine that one of the game consoles stolen from the 08/28/2018 GameStop robbery was sold to a pawn shop by Kaela McFadden, Kelvin McFadden's sister.

31. Based on records recovered from Sony, investigators were able to determine that the same game console pawned by Kaela McFadden was linked with a Sony Account associated with the online ID "KeezDaCapo." The KeezDaCapo account was created on 8/28/2018 and includes the listed name of Kelvin McFadden, the listed phone number of 443-890-7949, and the listed e-mail address of mcfaddenalijah2012@gmail.com. The mcfaddenalijah2012@gmail.com account was linked with the stolen PlayStation 4 as the "Sign-In ID".

32. Subscriber information records from TracFone for the phone number 443-890-7949 list Kelvin McFadden as the subscriber.

33. Investigators recovered a phone from Arnold's person after he was arrested for the attempted robbery of the Wawa on 7/22/2018. As mentioned above, two phones were recovered during a search warrant execution of McFadden's car after Williams and McFadden were arrested for the robbery of the GameStop on 9/1/2018.¹

34. Investigators confirmed that the phone recovered from Arnold, was in fact used by Arnold and belonged to him and was associated with 410-585-7592 by executing a search warrant on the phone.²

¹ Investigators obtained a state search warrant the search of the 2003 Honda Accord that was registered to McFadden and was involved in the high-speed chase following the final Gamestop robbery (9/1/2018). That search warrant also authorized state investigators to search for "Any and all cell phones" within the car and permitted them to undertake the "search and recovery, (download), of all data from within". For the purposes of this affidavit, federal investigators are not relying on any information or evidence obtained from the state download of the phones associated with Stewart Williams or Kelvin McFadden. I previously sought, and received, a federal search warrant for all three phones associated, respectively, with Stewart Williams, Kelvin McFadden, and Michael Arnold. 19-0559-JMC.

² State investigators obtained a warrant to search Arnold's phone and seize relevant evidence, fruits, and instrumentalities related to the robberies. While the state search of that phone yielded

19-2432 JMC -

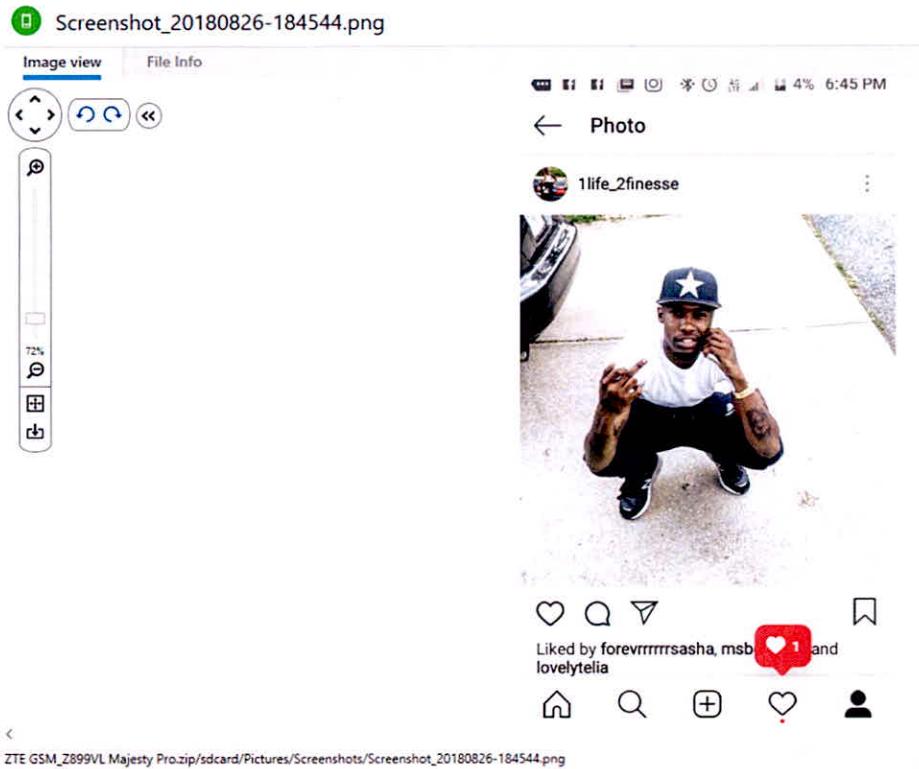
19-2435 JMC

DAL

35. On February 12, 2019, The Honorable J. Mark Coulson, United States Magistrate Judge for the District of Maryland, signed a warrant authorizing the search of three cell phones associated with Stewart Williams, Kelvin McFadden, and Michael Arnold, respectively, among other searches. *See* Misc. No. 19-0559-JMC.

36. After a search of the phone associated with Kelvin McFadden, I discovered pictures on the device of Kelvin McFadden, further leading me to believe that the device did in fact belong to Kelvin McFadden. Furthermore, the phone's extraction report lists 443-890-7949 as associated with the SIM card within the telephone.

37. A further search of this phone recovered the following picture of Kelvin McFadden, in a blue hat with a white star, associated with the "1life_2finesse" Instagram account.



38. Investigators obtained a warrant to search this Instagram account, which was in fact

information that is helpful to this investigation, I also sought and received a federal search warrant for the phone. 19-0559-JMC.

19-2432 JMC - 19-2435 JMC

DAL

linked to Kelvin McFadden. (19-1960-SAG.) Among other evidence, the search warrant return from Instagram included several videos that were linked with McFadden's Instagram account, and based on information from the returns, were posted by the account late in the day on August 25, 2018 or during the early morning hours of August 26, 2018. One such video depicts Stewart Williams dancing. Williams is wearing a black polo with a white logo that matches what a robber wore during a GameStop robbery on August 25, 2018. While dancing, Williams flashes a wad of U.S. currency. An Instagram user commented on the video "my n**** stew". A video posted later depicts McFadden and Williams dancing at a club while music is playing. Both are waving around wads of money. Another video, posted by McFadden's account later with the caption, "Almost caught this n****," depicts Williams sitting in the front seat of McFadden's car. The Instagram return also included numerous photographs of Kelvin McFadden. The account includes a picture of Stewart Williams in what appears to be Kelvin McFadden's car and several pictures of McFadden in a blue/navy "NB" new balance t-shirt that matches a shirt worn by a robber during the September 1 GameStop robbery.

39. The Instagram returns indicated that McFadden's Instagram account is linked with the e-mail address mcfaddenkelvin1993@gmail.com .

40. Records obtained from Apple show that mcfaddenkelvin1993@icloud.com is linked to and associated with "Kelvin McFadden" in Baltimore with a listed address of 1750 Montpelier Street. Records obtained from Apple also show that mcfaddenalijah2012@icloud.com is linked to and associated with "Kelvin McFadden" and "Alijah McFadden" and that Alijah McFadden's listed address is 1750 Montpelier Street. Public records indicate that Kelvin McFadden was born in 1993 and lists 1750 Montpelier Street as his address.

19-2432 JMC - 19-2435 JMC

DAL

Defendant Information**Defendant**

Name: **Mcfadden, Kelvin Richardo Jr.**
Race: **Black** **Sex:** **Male** **Height:** **6'2"** **Weight:** **165**
HairColor: **Black** **EyeColor:** **Brown**
DOB: **08/26/1993**
Address: **1750 Montpelier Street**
City: **Baltimore** **State:** **MD** **Zip Code:** **21218**

41. Records obtained from Apple indicate that Kelvin McFadden previously had an iPhone device registered in his name and associated with mcfaddenkelvin1993@icloud.com and associated with a phone number believed by investigators to have been linked to Kelvin McFadden.

42. Records obtained from Apple indicate that slw30@gmail.com is Stewart Williams's account and is linked to Williams's iPhone, which was the subject of a previously issued search warrant. (19-0559-JMC.)

CONCLUSION

43. Based on the above, I respectfully submit that there is probable cause to believe that Williams and McFadden have violated Title 18 U.S.C. § 1951(a) (Affecting Interstate Commerce by Robbery), and that there is probable cause to believe that evidence of these crimes, including potential photographs, communications, or information that links Kelvin McFadden, Stewart Williams, and/or Michael Arnold together or with other co-conspirators will be recovered from the information and records sought.

44. I respectfully request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

45. I respectfully request that the Court issue a search warrant to search the accounts listed in Attachments A-1, A-2, A-3, and A-4 and seize evidence, records, and items described in Attachments B-1, B-2, B-3, and B-4.

19 - 2432 JMC -

19 - 2435 JMC

DAL

46. Because the warrant will be served on Apple and Google who will then compile the information at a time convenient to them and because the warrant does not involve entry on to physical premises, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

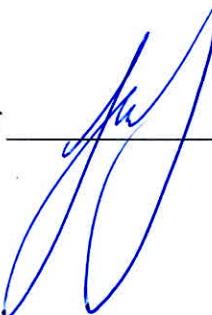
47. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

DAL

19 - 2432 JMC -

19 - 2435 JMC


Special Agent Brendan Plasha
Bureau of Alcohol, Tobacco, Firearms, and
Explosives

Subscribed to and sworn before me this 23 day of  , 2019

THE HONORABLE J. MARK COULSON
UNITED STATES MAGISTRATE JUDGE

FILED
LOGGED
ENTERED
RECEIVED
AUG 06 2019
AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND DEPUTY
EY

19 - 2432 JMC

DAL

ATTACHMENT A-1 TO SEARCH WARRANT

Apple, Inc.

Property to Be Searched

This warrant applies to information associated with the following Apple iCloud account:

- The Apple iCloud account associated with the email address

mcfaddenkelvin1993@icloud.com

The requested Apple iCloud information and records are stored at premises owned, maintained, controlled, or operated by Apple, Inc., a business headquartered at 1 Infinite Loop Cupertino, CA 95014.

19 - 2432 JMC

DAL

ATTACHMENT B-1 TO SEARCH WARRANT

Apple, Inc.

Particular Things to be Seized

I. Files and Accounts to be produced by Apple Inc. from January 1, 2018, to the present.

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of Apple (the “Target ISP”), the Target ISP is required to disclose the following information to the government for the accounts or identifiers listed in Attachment A-1 (the “Target Account”). Such information should include the below-described content of the subject account:

- a. All iCloud data existing on Apple’s servers, including subscriber information, mail logs, and all iCloud content, including, but not limited to, email, photo stream, photo library, documents, contacts, calendars, bookmarks, and Safari browsing history;
- b. All iOS device activation information and device backups, including photos and videos in the Camera Roll, device settings, app data, iMessage, SMS, and MMS messages and voicemail;
- c. All FaceTime records, including call invitation logs;
- d. All iMessage records, including capability query logs;
- e. All Find My iPhone records and transactional activity, including records of all attempts to locate, lock, or wipe the device;
- f. All My Apple ID, iForgot, and Game Center connection logs and transactional records;

- g. All device registration or customer information associated with the account, including name, address, email address, and telephone number;
- h. All customer service records, including support interactions, warranty and repair information;
- i. All iTunes data, including basic subscriber information, purchase information, and iTunes Match data;
- j. All Apple retail store, online store, and gift card information associated with the account;
- k. Subscriber Information, including the name and location, supplied by the user at the time of registration, the date the account was created and all of the services of the Target ISP used by the Target Account;
- l. Records of user activity for each connection made to or from the Target Account, including log files; messaging logs; the date, time, length, and method of connections; data transfer volume; user names; and source and destination Internet Protocol addresses, and any telephone, instrument or other unique identifiers collected by the Target ISP and associated with the Target Account;
- m. All telephone or instrument numbers associated with the Target Account (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network

Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”).

II. Information to be Seized by Law Enforcement Personnel

All information described above in Section I including correspondence, records, documents, photographs, videos, electronic mail, chat logs, and electronic messages that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §1951(a) (Affecting Interstate Commerce by Robbery) for the Target Account listed on Attachment A-1 and

a. Records, documents, programs, applications, photographs, video or audio recordings, call history information, text messages and other cellular phone communications, social media postings, stored phones numbers or address book contacts, voice mail messages or voice mails stored in any form, and other digital evidence, that refer or relate to:

- i. Firearms or items that appear to be firearms and weapons or items that appear to be weapons;
 - ii. KELVIN MCFADDEN and all associates of KELVIN MCFADDEN;
 - iii. Evidence of clothing worn during the commission of the offenses;
 - iv. Photographs of any items or object used during the commission of the offenses, including vehicles, bags, etc.;
 - v. Evidence or photographs related to stolen items, including U.S. currency and game systems;
 - vi. Finances, bank accounts, financial records, or records of financial transactions;
 - vi. Messages between KELVIN MCFADDEN and any associates.
- b. All phone books that contain and identify contacts of KELVIN MCFADDEN;

19 - 2432 JMC

c. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show the actual user(s), owner or possessor of the Target Account.

d. All location data, including any GPS coordinates or any applications that would store such information.

e. Evidence of who used, owned, or controlled the Target Account listed on Attachment A-1.

g. Evidence of the times the Target Account listed on Attachment A-1 was used.

h. Passwords and encryption keys, and other access information that may be necessary to access the Target Account listed on Attachment A-1 and other associated accounts.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage and any photographic form.

III. The government's search

With respect to the search of the information provided pursuant to this warrant by the above-referenced provider, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically-stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

FILED
LOGGED
ENTERED
RECEIVED
AUG 06 2019
AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
DEPUTY
CY

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS
RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Apple, Inc. (hereinafter "Apple"), and my official title is _____. I am a custodian of records for Apple. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Apple, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Apple; and
- c. such records were made by Apple as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature

19-2433 JMC

DAL

ATTACHMENT B-2 – Google, LLC**I. Files and Accounts to be produced by Google, LLC between January 1, 2018 and the present**

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of Google, LLC including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Google or have been preserved pursuant to a preservation request under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for each account or identifier listed in Attachment A-2:

A. Google Account Information

1. Google account registration information, including name, user-specified contact information, recovery email address, recovery SMS number, account creation timestamp and IP address, and a list of Google services the account holder has enabled or accessed;
2. Account change history IP addresses and associated timestamps;
3. Google account login and logout IP addresses and associated timestamps;
4. All means and sources of payment for all Google products and services (including complete credit or bank account numbers), and detailed billing records;
5. All cookie and user-specific advertising data, including third-party cookies;

B. Gmail Account Information

6. Gmail specific subscriber information, login and logout IP addresses and associated timestamps;
7. Gmail specific non-content email header information, originating message IP addresses, and account settings;
8. The contents of all e-mails, attachments and chat messages stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination e-mails sent addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
9. Contents of all available deleted emails;

C. YouTube Account Information

10. YouTube specific subscriber information, including date of birth and country;
11. YouTube specific login and logout IP addresses and associated timestamps;
12. YouTube video upload IP addresses and associated timestamps;

19 - 2433 JMC

13. Copies of all publically available videos;
14. Copies of all private videos and associated video information;
15. Copies of all private messages;
16. All Channel or Video comments;
17. All contacts;

D. Google Voice Account Information

18. Voice specific subscriber information, including signup IP and associated timestamp and user-provided name;
19. Most recent 28 days of call and text logs;
20. All account settings and account change history;
21. Contents of all voicemail messages and text messages;

E. Blogger Account Information

22. Blogger specific subscriber information, including Blog registration information, Blog creation IP and timestamp, Blog owner/admin subscriber information, and post or comment owner information;
23. All contents of private blog posts and comments;

F. Google+ Account Information

24. Google+ specific subscriber and IP address information, including associated timestamps;
25. All IP addresses and timestamps associated with Posts, Comments, or Photos;
26. All Content/Activity Stream, including posts, comments, and photos;
27. All contacts/Circles;
28. Google+ Profiles;

G. Android Account Information

29. Android specific subscriber and IP address information, including associated timestamps;
30. All device IDs, IMEIs, and MEIDs associated with the target account(s);

19 - 2433 JMC

31. Timestamps, including device registration, first check-in, and last check-in;
32. All Google accounts tied to the Android device(s) if any;
33. Android hardware information;
34. Cell carrier/service provider;
35. All apps downloaded to the device;

H. Photos Account Information

36. Photos specific subscriber and IP address information, including associated timestamps;
37. All upload IP addresses and associated timestamps;
38. Contents of all Photos and Albums, including all exif data included by the user as part of the upload;

I. Drive Account Information

39. Drive specific subscriber and IP address information, including associated timestamps;
40. All upload IP addresses and associated timestamps;
41. All Drive content, including Docs, Sheets and Slides;

J. Google Location and Search History Information

42. All location history with associated timestamps on the dates listed below:

	Date
1	5/24/2018 to 5/26/2018
2	6/9/2018 to 6/11/2018
3	6/19/2018 to 6/21/2018
4	7/9/2018 to 7/12/2018
5	7/17/2018 to 7/21/2018

6	7/21/2018 to 7/23/2018
7	7/25/2018 to 7/27/2018
8	8/4/2018 to 8/6/2018
9	8/17/2018 to 8/19/2018
10	8/20/2018 to 8/22/2018
11	8/24/2018 to 8/26/2018
12	8/27/2018 to 8/29/2018
13	8/31/2018 to 9/01/2018

43. All search history and associated timestamps, including all “clicks” and “queries;”

K. Waze Location and Search History Information

44. Waze specific subscriber information, login and logout IP addresses and associated timestamps;

45. Waze specific non-content information, including account settings;

46. All location history with associated timestamps on the dates listed below:

	Date
1	5/24/2018 to 5/26/2018
2	6/9/2018 to 6/11/2018
3	6/19/2018 to 6/21/2018
4	7/9/2018 to 7/12/2018
5	7/17/2018 to 7/21/2018

FILED
 LOGGED
 AUG 06 2019
 CLERK US DISTRICT COURT
 DISTRICT OF MARYLAND DEPUTY
 EY

19 - 2433 JMC

DAL

6	7/21/2018 to 7/23/2018
7	7/25/2018 to 7/27/2018
8	8/4/2018 to 8/6/2018
9	8/17/2018 to 8/19/2018
10	8/20/2018 to 8/22/2018
11	8/24/2018 to 8/26/2018
12	8/27/2018 to 8/29/2018
13	8/31/2018 to 9/01/2018

47. All Waze search history and associated timestamps, including all “clicks” and “queries;”

48. All Waze locations saved by the user;

II. Information to be Seized by Law Enforcement Personnel

a. Any and all records that relate in any way to the account described in Attachment A-2 which is evidence, fruits, and instrumentalities of violations of 18 U.S.C. §1951(a) (Affecting Interstate Commerce by Robbery).including:

1. All records, information, documents or tangible materials related to Affecting Interstate Commerce by Robbery or the sale of ill-gotten proceeds thereof, including the sale of any stolen Game Systems or other merchandise; any and all communications related to the preparation for or completion of the robberies or the sale of the proceeds thereof.
- b. All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of these crimes;
- c. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts;
- d. Evidence of the times the account was used;

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS
RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google LLC. (hereinafter "Google"), and my official title is _____. I am a custodian of records for Google. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Google; and
- c. such records were made by Google as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature

19 - 2434 JMC

DAL

ATTACHMENT A-3 – Google, LLC

This warrant applies to information associated with the Google account mcfaddenlijah2012@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google, LLC, a business with offices located at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B-3 – Google, LLC**II. Files and Accounts to be produced by Google, LLC between January 1, 2018 and the present**

To the extent that the information described in Attachment A-3 is within the possession, custody, or control of Google, LLC including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Google or have been preserved pursuant to a preservation request under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for each account or identifier listed in Attachment A-3:

A. Google Account Information

1. Google account registration information, including name, user-specified contact information, recovery email address, recovery SMS number, account creation timestamp and IP address, and a list of Google services the account holder has enabled or accessed;
2. Account change history IP addresses and associated timestamps;
3. Google account login and logout IP addresses and associated timestamps;
4. All means and sources of payment for all Google products and services (including complete credit or bank account numbers), and detailed billing records;
5. All cookie and user-specific advertising data, including third-party cookies;

B. Gmail Account Information

6. Gmail specific subscriber information, login and logout IP addresses and associated timestamps;
7. Gmail specific non-content email header information, originating message IP addresses, and account settings;
8. The contents of all e-mails, attachments and chat messages stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination e-mails sent addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
9. Contents of all available deleted emails;

C. YouTube Account Information

10. YouTube specific subscriber information, including date of birth and country;
11. YouTube specific login and logout IP addresses and associated timestamps;
12. YouTube video upload IP addresses and associated timestamps;

19-2434 JMC

13. Copies of all publically available videos;
14. Copies of all private videos and associated video information;
15. Copies of all private messages;
16. All Channel or Video comments;
17. All contacts;

D. Google Voice Account Information

18. Voice specific subscriber information, including signup IP and associated timestamp and user-provided name;
19. Most recent 28 days of call and text logs;
20. All account settings and account change history;
21. Contents of all voicemail messages and text messages;

FILED _____ ENTERED _____
LOGGED _____ RECEIVED _____
AUG 06 2019

E. Blogger Account Information

22. Blogger specific subscriber information, including Blog registration information, Blog creation IP and timestamp, Blog owner/admin subscriber information, and post or comment owner information;

AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND DEPUTY

23. All contents of private blog posts and comments;

F. Google+ Account Information

24. Google+ specific subscriber and IP address information, including associated timestamps;
25. All IP addresses and timestamps associated with Posts, Comments, or Photos;
26. All Content/Activity Stream, including posts, comments, and photos;
27. All contacts/Circles;
28. Google+ Profiles;

G. Android Account Information

29. Android specific subscriber and IP address information, including associated timestamps;
30. All device IDs, IMEIs, and MEIDs associated with the target account(s);

31. Timestamps, including device registration, first check-in, and last check-in;
32. All Google accounts tied to the Android device(s) if any;
33. Android hardware information;
34. Cell carrier/service provider;
35. All apps downloaded to the device;

H. Photos Account Information

36. Photos specific subscriber and IP address information, including associated timestamps;
37. All upload IP addresses and associated timestamps;
38. Contents of all Photos and Albums, including all exif data included by the user as part of the upload;

I. Drive Account Information

39. Drive specific subscriber and IP address information, including associated timestamps;
40. All upload IP addresses and associated timestamps;
41. All Drive content, including Docs, Sheets and Slides;

J. Google Location and Search History Information

42. All location history with associated timestamps on the dates listed below:

	Date
1	5/24/2018 to 5/26/2018
2	6/9/2018 to 6/11/2018
3	6/19/2018 to 6/21/2018
4	7/9/2018 to 7/12/2018
5	7/17/2018 to 7/21/2018

6	7/21/2018 to 7/23/2018
7	7/25/2018 to 7/27/2018
8	8/4/2018 to 8/6/2018
9	8/17/2018 to 8/19/2018
10	8/20/2018 to 8/22/2018
11	8/24/2018 to 8/26/2018
12	8/27/2018 to 8/29/2018
13	8/31/2018 to 9/01/2018

43. All search history and associated timestamps, including all “clicks” and “queries;”

K. Waze Location and Search History Information

44. Waze specific subscriber information, login and logout IP addresses and associated timestamps;

45. Waze specific non-content information, including account settings;

46. All location history with associated timestamps on the dates listed below:

	Date
1	5/24/2018 to 5/26/2018
2	6/9/2018 to 6/11/2018
3	6/19/2018 to 6/21/2018
4	7/9/2018 to 7/12/2018
5	7/17/2018 to 7/21/2018

6	7/21/2018 to 7/23/2018
7	7/25/2018 to 7/27/2018
8	8/4/2018 to 8/6/2018
9	8/17/2018 to 8/19/2018
10	8/20/2018 to 8/22/2018
11	8/24/2018 to 8/26/2018
12	8/27/2018 to 8/29/2018
13	8/31/2018 to 9/01/2018

47. All Waze search history and associated timestamps, including all “clicks” and “queries;”

48. All Waze locations saved by the user;

II. Information to be Seized by Law Enforcement Personnel

j. Any and all records that relate in any way to the account described in Attachment A-3 which is evidence, fruits, and instrumentalities of violations of 18 U.S.C. §1951(a)) (Affecting Interstate Commerce by Robbery).including:

2. All records, information, documents or tangible materials related to Affecting Interstate Commerce by Robbery or the sale of ill-gotten proceeds thereof, including the sale of any stolen Game Systems or other merchandise; any and all communications related to the preparation for or completion of the robberies or the sale of the proceeds thereof.

k. All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of these crimes;

l. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts;

m. Evidence of the times the account was used;

19 - 2434 JMC

DAL

- n. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
- o. Passwords and encryption keys, and other access information that may be necessary to access the account and other associated accounts;
- p. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;
- q. All existing printouts from original storage which concern the categories identified in subsection II.A; and
- r. All "address books" or other lists of contacts.

III. The government's search

With respect to the search of the information provided pursuant to this warrant by the above-referenced provider, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically-stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS
RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google LLC. (hereinafter "Google"), and my official title is _____. I am a custodian of records for Google. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Google; and
- c. such records were made by Google as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature

FILED
LOGGED
ENTERED
RECEIVED
AUG 06 2019
AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND DEPUTY

19 - 2435 JMC

ATTACHMENT A-4 – Google, LLC

This warrant applies to information associated with the Google account slw30@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google, LLC, a business with offices located at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

19-2435 JMC

ATTACHMENT B-4 – Google, LLC**III. Files and Accounts to be produced by Google, LLC between January 1, 2018 and the present**

To the extent that the information described in Attachment A-4 is within the possession, custody, or control of Google, LLC including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Google or have been preserved pursuant to a preservation request under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for each account or identifier listed in Attachment A-4:

A. Google Account Information

1. Google account registration information, including name, user-specified contact information, recovery email address, recovery SMS number, account creation timestamp and IP address, and a list of Google services the account holder has enabled or accessed;
2. Account change history IP addresses and associated timestamps;
3. Google account login and logout IP addresses and associated timestamps;
4. All means and sources of payment for all Google products and services (including complete credit or bank account numbers), and detailed billing records;
5. All cookie and user-specific advertising data, including third-party cookies;

B. Gmail Account Information

6. Gmail specific subscriber information, login and logout IP addresses and associated timestamps;
7. Gmail specific non-content email header information, originating message IP addresses, and account settings;
8. The contents of all e-mails, attachments and chat messages stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination e-mails sent addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

9. Contents of all available deleted emails;

AUG 06 2019

C. YouTube Account Information

10. YouTube specific subscriber information, including date of birth and country;
11. YouTube specific login and logout IP addresses and associated timestamps;
12. YouTube video upload IP addresses and associated timestamps;

19 - 2435 JMC

DAL

13. Copies of all publically available videos;
14. Copies of all private videos and associated video information;
15. Copies of all private messages;
16. All Channel or Video comments;
17. All contacts;

D. Google Voice Account Information

18. Voice specific subscriber information, including signup IP and associated timestamp and user-provided name;
19. Most recent 28 days of call and text logs;
20. All account settings and account change history;
21. Contents of all voicemail messages and text messages;

E. Blogger Account Information

22. Blogger specific subscriber information, including Blog registration information, Blog creation IP and timestamp, Blog owner/admin subscriber information, and post or comment owner information;

23. All contents of private blog posts and comments;

F. Google+ Account Information

24. Google+ specific subscriber and IP address information, including associated timestamps;
25. All IP addresses and timestamps associated with Posts, Comments, or Photos;
26. All Content/Activity Stream, including posts, comments, and photos;
27. All contacts/Circles;
28. Google+ Profiles;

G. Android Account Information

29. Android specific subscriber and IP address information, including associated timestamps;
30. All device IDs, IMEIs, and MEIDs associated with the target account(s);

31. Timestamps, including device registration, first check-in, and last check-in;
32. All Google accounts tied to the Android device(s) if any;
33. Android hardware information;
34. Cell carrier/service provider;
35. All apps downloaded to the device;

H. Photos Account Information

36. Photos specific subscriber and IP address information, including associated timestamps;
37. All upload IP addresses and associated timestamps;
38. Contents of all Photos and Albums, including all exif data included by the user as part of the upload;

I. Drive Account Information

39. Drive specific subscriber and IP address information, including associated timestamps;
40. All upload IP addresses and associated timestamps;
41. All Drive content, including Docs, Sheets and Slides;

J. Google Location and Search History Information

42. All location history with associated timestamps on the dates listed below:

	Date
1	5/24/2018 to 5/26/2018
2	6/9/2018 to 6/11/2018
3	6/19/2018 to 6/21/2018
4	7/9/2018 to 7/12/2018
5	7/17/2018 to 7/21/2018

6	7/21/2018 to 7/23/2018
7	7/25/2018 to 7/27/2018
8	8/4/2018 to 8/6/2018
9	8/17/2018 to 8/19/2018
10	8/20/2018 to 8/22/2018
11	8/24/2018 to 8/26/2018
12	8/27/2018 to 8/29/2018
13	8/31/2018 to 9/01/2018

43. All search history and associated timestamps, including all “clicks” and “queries;”

K. Waze Location and Search History Information

44. Waze specific subscriber information, login and logout IP addresses and associated timestamps;

45. Waze specific non-content information, including account settings;

46. All location history with associated timestamps on the dates listed below:

	Date
1	5/24/2018 to 5/26/2018
2	6/9/2018 to 6/11/2018
3	6/19/2018 to 6/21/2018
4	7/9/2018 to 7/12/2018
5	7/17/2018 to 7/21/2018

6	7/21/2018 to 7/23/2018
7	7/25/2018 to 7/27/2018
8	8/4/2018 to 8/6/2018
9	8/17/2018 to 8/19/2018
10	8/20/2018 to 8/22/2018
11	8/24/2018 to 8/26/2018
12	8/27/2018 to 8/29/2018
13	8/31/2018 to 9/01/2018

47. All Waze search history and associated timestamps, including all “clicks” and “queries;”

48. All Waze locations saved by the user;

II. Information to be Seized by Law Enforcement Personnel

s. Any and all records that relate in any way to the account described in Attachment A-4 which is evidence, fruits, and instrumentalities of violations of 18 U.S.C. §1951(a)) (Affecting Interstate Commerce by Robbery).including:

3. All records, information, documents or tangible materials related to Affecting Interstate Commerce by Robbery or the sale of ill-gotten proceeds thereof, including the sale of any stolen Game Systems or other merchandise; any and all communications related to the preparation for or completion of the robberies or the sale of the proceeds thereof.

t. All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of these crimes;

u. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts;

v. Evidence of the times the account was used;

19 - 2435 JMC

w. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;

x. Passwords and encryption keys, and other access information that may be necessary to access the account and other associated accounts;

y. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;

z. All existing printouts from original storage which concern the categories identified in subsection II.A; and

aa. All "address books" or other lists of contacts.

III. The government's search

With respect to the search of the information provided pursuant to this warrant by the above-referenced provider, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically-stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS
RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google LLC. (hereinafter "Google"), and my official title is _____. I am a custodian of records for Google. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Google; and
- c. such records were made by Google as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature

FILED _____ ENTERED _____
LOGGED _____ RECEIVED _____
AUG 06 2019